

CSO

THE RESOURCE FOR SECURITY EXECUTIVES

SURVEILLANCE SUNDAY

Friendly's CSO uses CCTV to dish out praise PAGE 26

LOPHT IN TRANSITION

Famous hacking group then and now PAGE 30



Hazy Skies for PCI?

The Payment Card Industry security standard is a critical attempt at self-regulation. But right now, PCI compliance is slow and murky.

By Sarah D. Scalet PAGE 16

John Kirkwood, CISO of Royal Ahold, says PCI needs a more unified standard.



MULTIPLY SECURITY
AND MAXIMIZE UPTIME.



INTEL® VPRO™ TECHNOLOGY WITH INTEL® CORE™2 DUO PROCESSOR.
Manage smarter. Repair PCs or deploy security upgrades remotely, even if they're powered off.*
Automatically isolate an infected desktop from the network before it infects other PCs. With 64-bit
capable Intel vPro technology you multiply your company's possibilities. **Learn more at intel.com/vPro**



Intel® Active Management Technology (AMT) requires the platform to have an Intel® AMT-enabled chipset, network hardware and software, connection with a power source and a network connection.
© 2007 Intel Corporation. Intel, the Intel logo, Intel Core, the Intel Core logo, Intel Leap ahead, Intel vPro and the Intel Leap ahead, and vPro logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. All rights reserved.

contents

April 2007

Vol. 6, No. 4

Features

16 COVER STORY Standardized Tests

PCI COMPLIANCE More than just another data-security standard, the PCI program is corporate America's most ambitious effort yet to prove that it can self-regulate. But even a standard with everything going for it might not be enough to stop the loss of credit card data. *By Sarah D. Scalet*

22 The Scourge of Image Spam

SPAM EVOLUTION How the latest iteration of junk mail is beating filters and filling inboxes. *By Scott Berinato*

26 The Scoop on Loss Prevention

LOSS PREVENTION Friendly's Restaurants' Ernie Patnode approaches cash management with a lot of common sense, a little technology and, yes, politeness. *By Scott Berinato*

30 LOpht in Transition

INFORMATION SECURITY Most of the '90s hacking group have emerged in legitimate roles. Was their work ultimately boon or bane for security? *By Michael Fitzgerald*

ERNIE PATNODE,
security chief at Friendly's
Restaurants, looks to use
surveillance of employees
so he can dish out praise
when they prevent losses.

COLUMNS

14 Protecting the \$100 Laptop

MACHINE SHOP The ultracheap computing device for developing nations presents unique security challenges. *By Simson Garfinkel*

DEPARTMENTS

7 Briefing

10 rules for responsible investigations; Trouble in movie city; Changing on the fly; FTC Chief: Adware beware; The Security Blotter; How to calm someone in a crisis

36 Debriefing

Smuggler's Notch: Stashed and Found

IN EVERY ISSUE

- 2 CSOonline.com
- 4 From the Editor
- 31 Index





What Metal Theft Looks Like

We heard from a number of security executives who nodded their heads about our February story "Red Gold Rush," describing a metal theft epidemic. Go to CSOonline.com to view a slidecast that vividly shows what metal theft looks like. Written by Senior Editor **Scott Berinato**. www.csoonline.com/read/020107/fea_metal/slide01.html

NEW BLOGGERS

Perry Carpenter, an information security and privacy practitioner who's worked on infosecurity projects at Wal-Mart and Sam's Club, brings an experienced eye to **SECURITY SMACK-DOWN**. **Phil Becker** and **Eric Norlin** tackle trends related to identity management in **DIGITAL ID WORLD**. Find all of our bloggers at blogs.csoonline.com.

Speaking of Bloggers...

One of our most popular online pieces in recent memory was "How to Crash an In-Flight Entertainment System," by security consultant **Hugh Thompson** on his blog, **SECURITY SAMURAI**. Read it, and the many comments this piece evoked, at blogs.csoonline.com/node/151.

"How is it that Mozilla, Apple and others have, for so long, gotten away with claiming moral superiority in the security space over Microsoft? It seems that Microsoft's rivals made security a marketing platform—bad move, IMHO."

—PERRY CARPENTER, IN HIS SECURITY SMACK-DOWN BLOG, BLOGS.CSOONLINE.COM/BLOG/PERRY_CARPENTER

CSO

President and CEO
Michael Friedenberg
Publisher Bob Bragdon

EDITORIAL

Editor in Chief Derek Slater
Managing Editor
Michael Goldberg
Senior Editors
Scott Berinato, Sarah D. Scalet
Editor at Large Simson Garfinkel
Assistant Managing Editor
Emily S. Henderson
Senior Copy Editor
Cathy Mallen
Copy Editor
Susan Bryant-Still
Associate Staff Writers
Christopher Lynch, Katherine Walsh
Editorial Administrator
Jill Paquette
Contributors
Michael Fitzgerald,
Robert McMillan, Deb Radcliff

DESIGN

Executive Director, Art and
Design Mary Lester
Art Director Steve Traynor
Associate Art Director
Chandra Tallman

RESEARCH

Research Manager
Carolyn Johnson
Senior Research Analyst
Seanna Maguire

ONLINE EDITORIAL

Online Editorial Director
Christopher Lindquist
Senior Online Editors
Sandy Kendall, Meredith Levinson,
Shawna McAlearney,
Esther Schindler
Associate Online Editor
Diann Daniel
Online News Writer Al Sacco
Online Copy Editor David Gradjan

INFORMATION SYSTEMS

IDG Director of Information
Services Nancy Newkirk
IT Manager Sean McCracken
Senior User Support Specialists
Christopher A. Kay,
Thomas Lupien
User Services Specialist
Gloria Lam
Associate User Support Specialist
James Brevard
Senior Web Developer
David Cohen
Web Developer Sanghee Seo

CXO MEDIA / IDG

COO Matt Smith
CSO Robert Hayes

 CXO MEDIA INC.

INTERNATIONAL DATA GROUP

Board Chairman
Patrick J. McGovern
President, IDG Communications
Bob Carrigan

 **BPA**
WORLDWIDE™



Passion | Expertise | Trust

Trust is being objective and doing what's right.
Trust is fulfilling promises made to our clients.
We're more than a vendor. **We're a true security partner.**

SecureWorks®
LURHQ™

LURHQ and SecureWorks have merged to become the most effective managed security services provider.
Get more info at: <http://www.secureworks.com> | 877.905.6661 | info@secureworks.com

Security Device Management | Enterprise Security Monitoring | Security Information and Event Management
Vulnerability Scanning | Threat Intelligence | Professional Services | E-mail Encryption



The Age of Analytics

Once upon a time I interviewed Dr. Hans Berliner. Berliner was a computer science professor at Carnegie Mellon and also a world champion at correspondence chess. Combin-

ing these two interests, he'd created a chess-playing program called Hitech.

At the time (in 1990), computers were horrible at chess. Slow and bad. Most programmers were concerned with writing selective search algorithms. That means they wanted the computers to play "like a human," focusing their processing cycles on analyzing a small set of plausible moves, rather than wasting time considering the ramifications of moves that, to human players, were obviously bad from the get-go.

Berliner said that a brute force approach was actually much more interesting. He said that a computer examining every single possibility could find surprisingly powerful move sequences among those many ideas that humans automatically reject. Berliner's research indicated that this was true in chess, and in games like *Go* and various other computational challenges.

In other words, once you give it enough horsepower, a computer is better off playing "like a computer" than like a human. Time has proven Berliner correct. Today's best chess programs play moves that look unnatural to the human player but that are in fact quite strong.

We've hit that tipping point in video surveillance systems—the point where computers, through brute force, can routinely and automatically find things in video that people can't. I think of it as entering the age of analytics. For some time it's been possible to capture and store gigabytes, terabytes, even petabytes of video. Now software systems can efficiently analyze all that data, looking for unexpected movement, unanticipated patterns,

familiar faces, customer behavior and more. Seems like we run across another new surveillance vendor every day, and the big camera system vendors also are building in more intelligence with each generation of their management software. (Even as I was writing this article, news appeared in my inbox about Honeywell's purchase of an analytics purveyor called ActivEye.) In addition to the security benefits, these new analytical video systems—intelligently deployed and managed—can help the security function deliver added intelligence to the business to improve workflow, enhance product quality, measure the effectiveness of promotions and marketing, and more.

Happily, the increased role of computation doesn't mean that people will be phased out of the surveillance equation completely. It just means that instead of glazing over staring at screen after screen, people can apply their intelligence where it's most useful. It turns out that the machines now have the horsepower to make old-time security systems into something much more than ever before.

—Derek Slater, dslater@cxo.com

HOW TO REACH US E-mail csletters@cxo.com Phone 508 872-0080 Fax 508 879-7784 Address CSO Magazine, 492 Old Connecticut Path, P.O. Box 9208, Framingham, MA 01701-9208; Subscriber Services Phone 866 354-1125 Fax 847 564-9453 E-mail csletters@omeda.com; Reprints For article reprints (100 quantity or more), contact Keith Williams at PARS International at 212 221-9595 x319 or e-mail keith.williams@parsintl.com.

ABOUT IDG International Data Group (IDG), the leading global provider of IT media, research, conferences and events, informs more people about technology than any other company in the world. Offering the widest range of media options, IDG reaches more than 120 million technology buyers in 85 countries representing 95 percent of worldwide IT spending. IDG publishes more than 300 newspapers and magazines in 85 countries, led by the *Computerworld*, *Infoworld*, *Macworld*, *Network World*, *PC*

World and *CIO* global product lines. IDG offers online users the largest network of technology-specific sites around the world through [IDG.net](http://www.idg.net) (www.idg.net), a gateway to IDG's 330 websites powered by more than 2,000 journalists reporting from every continent in the world. IDG also produces 168 technology-related conferences and events, and research company IDC provides global market intelligence, analysis and forecasts in 43 countries.

We do not come in peace.

They want you to spend months installing security and systems management in your organization. And then take days or even weeks to protect less than 60% of your systems. Boy is that stupid! Cyberattacks start and finish in minutes, not days.

Whether you're captain of Starship Enterprise—or just an enterprise—ask your chief

security officer how long it takes to inoculate and verify that every computer is secure. If it takes more than a few minutes, execute somebody.

BFG
(BigFix Gun)
defensive weaponry routinely protects hundreds of thousands of computers in minutes, not weeks. Give us 3 hours to demonstrate the projection of real power, free to qualified enterprises. We'll train your people, install a BFG behind your firewall, and then treat everyone to lunch. When we get back, we're betting you won't let us uninstall. Especially if you are a Symantec/Altiris customer!

Schedule a demo via www.bigfix.com/bfg, or call 510-652-6700 x116. We'll also send you a color poster of this ad.

 **BIGFIX®**
Never before have so few done so much, so fast, for so many.

©2007 BIGFIX. BIGFIX and its logo are registered trademarks of BIGFIX, Inc. All other trademarks are acknowledged ... with extreme prejudice. Illustration by Daryl Mandryk.

IRBA



The new iCLASS readers:

Price ► same as Prox.

Installation ► same as Prox.

Power Requirement ► same as Prox.

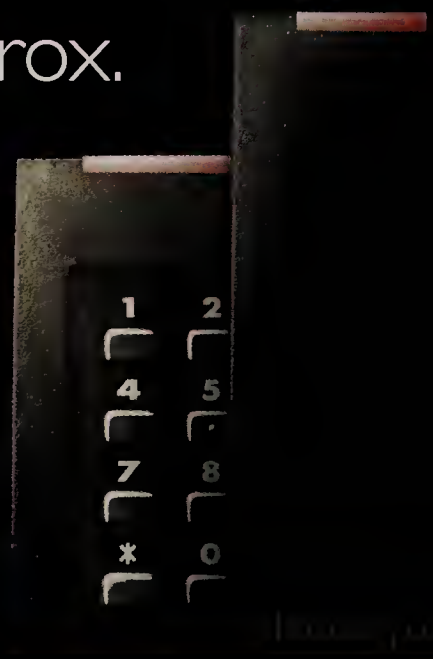
Security ► same as Alcatraz.

iCLASS readers offer enhanced security with all the user-friendly features of proximity.

The new iCLASS readers are virtually identical to proximity – in power requirement, ease of use and installation, even price. The only difference is that iCLASS offers enhanced security through encryption and mutual authentication, and its read/write capabilities allow you to add functionality such as biometrics, time and attendance, PC log-on security and more. Plus iCLASS comes from HID. So there's a lot to feel secure about.

ACCESS security.

iCLASS



briefing

News, Stats and Fast Facts Edited by Michael Goldberg

10 Rules for Responsible Investigations

Readers' best practices for making sure the sleuth work matches the allegation

INVESTIGATIONS How do you run a responsible investigation, one that's done not only in a legal and ethical way (of course that's a prerequisite) but that's also effective? To find out, and as a follow-up to our analysis of Hewlett-Packard's recent troubles over its inquiry into boardroom leaks (see www.csoonline.com/010107), we asked readers of CSOonline.com. We posted a preliminary list of best practices at Disclosures, the blog from CSO's editors (blogs.csoonline.com/blog/cso_editors), and invited readers to add their own. Below, the results. —Sarah D. Scalet



5) Match the investigatory methods to your corporate culture.

There's a huge gray area of ethics in investigations. Make sure that what you're doing makes sense for your company and follows practices that your CEO would be willing to defend on camera.

6) Be consistent. Don't treat a high-performing employee different from the slacker for the same offense. Apply even standards in how you manage contractors and subcontractors. Ensure that whatever practice you use is well documented, can be replicated and can be presented to opposing counsel.

7) Practice strict "need to know" rules during the investigation. Don't allow allegations to ruin someone's reputation. Expand the base of people involved only when absolutely necessary, even at the expense of ruffling some senior corporate egos. There will be plenty of time to brief people once the allegations are confirmed.

8) Make sure employees know their rights. Your personnel policy should state clearly that phone conversations on company phones and data that traverses the company network or company equipment is the property of the company and as such may be monitored, tracked and audited.

9) Decide when to tell the subject of an investigation. Have a formal policy for when those under investigation will (or will not) be notified.

10) Plan for possible mistakes. Have a process in place for people to raise concerns about how an investigation is being run. And make sure the process works.

1) Don't break the law. Don't hire anyone (or hire anyone who will hire anyone) who will break the law.

2) Before you start, agree on some general objectives. What do you want to accomplish? Set milestones to measure your progress. The overarching goal, of course, is to protect the corporation—both from whatever allegation you're investigating and from the possible repercussions of how you investigate it.

3) Seek the truth. Don't start with a preconceived outcome and try to make the facts fit—even if it is more convenient for the company.

4) Match the investigation to the crime. Don't launch a \$10,000 investigation into a \$1,000 crime. Beware of a tendency to hit the ground running to catch the bad guys quickly, which could result in an investigation that veers off course and creates a larger issue than the reason the investigation was started in the first place.

Trouble in Movie City

Global piracy cost Los Angeles County manufacturers an estimated \$5.2 billion in 2005, according to the Los Angeles County Economic Development Corp. Trade in pirated goods diverted another \$2 billion from the region's retail sector. Here's a breakdown of 2005 losses in millions of dollars due to counterfeiting in the area.

INSCRUTABLE TERM OF THE MONTH

ram raid (ram rād)

Noun: 1. A method of theft in which a heavy vehicle is driven through a wall, door or window of a facility to gain access to valuables. A destructive smash-and-grab theft using a steel cable attached to a heavy vehicle on one side and hooked to a cash source such as a safe on the other. The vehicle is driven forward to drag the safe out of the facility.

Verb: To crash a vehicle into a facility to steal valuables.

Forms: ram raiding, ram raided

Example: In the failed Millennium Dome robbery in 2000, thieves seeking diamonds ram raided the Greenwich, England, landmark with a bulldozer.

SOURCES: BBC, WIKIPEDIA, SYDNEY MORNING HERALD

Movie production **\$2,748**

Sound recording **\$851**

Apparel, accessories, footwear **\$617**

Software publishing **\$355**

Dolls, toys, games **\$275**

Drugs **\$132**

Aerospace parts, equipment **\$89**

Athletic goods **\$74**

Auto parts **\$38**

SOURCE: LOS ANGELES COUNTY ECONOMIC DEVELOPMENT CORP., FEB. 2007 REPORT

Oracle Fusion Middleware

Industry Leaders Rely On Oracle Identity Management

BRITISH AIRWAYS 

 *Ingersoll Rand*

 QUALCOMM®

 SAMSUNG
ELECTRONICS

Oracle Fusion Middleware

Hot-Pluggable. Comprehensive.

Single Sign-on — Access Management — Identity Administration — User Provisioning — Federated Identity
Virtual Directory — LDAP Directory — Web Services Management

ORACLE®

oracle.com/middleware
or call 1.800.ORACLE.1

Changing on the Fly

Polymorphic malware changes shape to fool detection schemes

When CISOs talk about polymorphic malware, they'll remind you that polymorphism is nothing new. Known to researchers since the 1980s, this malicious code changes its attributes to make it undetectable by signature- and behavior-based antivirus and intrusion detection defenses.

Ten years ago, at the annual Defcon hacker conference, push-button-simple server-side polymorphic features were introduced with the Back Orifice 2.0 backdoor Trojan. Then came an outbreak of polymorphic worms in the early 2000s (Code Red, Nimda and SirCam). Then talk of them quieted.

Now polymorphic malware is being used to send multiple variants of Trojans, and bots are being sent out in short "bursts," that last an hour or less and are gone before detection systems vendors even have a chance to write a signature, says Amir Lev, president of Commtouch, an Israeli-based OEM vendor of a widely used virus detection engine called Recurrent Pattern Detection technology.

One example is the Storm Worm, a spam e-mail attachment that broke out in January with subject lines such as "230 dead as storm batters Europe." Commtouch detected "tens of thousands of variants" of this spam message in January, Lev says. Another example is the Stration family of malware, responsible for worms and other forms of malware in late 2006. "Stration was changing so quickly—the encryption packaging, the compiler, everything. We saw up to 300 variants



in a single day," says Ron O'Brien, senior security analyst at anti-malware vendor Sophos.

The fight against polymorphic malware is an arms race: the bad guys against you and your security

vendors. Vendors continue to add new scanning capability to their engines, which commonly include pre- and post-scanning of executable files in search

of payloads and programming routines indicative of malware. The engines do this scanning in a controlled environment, or "sandbox." This scan uses a heuristic routine or behavior analysis to detect potential problems. So, for example, if the executable checks to see what antivirus engine is running, or if it tries to contact the master controller, some scanning technolo-

gies would detect and block that, O'Brien explains.

Such a technique of scanning executable files "doesn't work with today's botware because when you try to run them in the sandbox, zombies won't do anything," Lev explains. "Later on, they'll try to contact the master controller, but they do that when the computer is idle, usually late at night."

Besides deploying intrusion prevention and anti-malware systems that use heuristics, your network defenses should include a layer of scanning that looks for potential malware variants. For example, polymorphic applications often use their own style of file compression formats because the encryption can be changed on the fly. A well-executed defense would flag such a file as suspect.

You also need to tune your network detection to work in real-time. "You must rely on layers of scanning and zero-hour protection and response," Lev says.

—Deb Radcliff



FTC Chief: Adware Beware

SPYWARE In the past year, the Federal Trade Commission reached settlements with spammers, adware distributors and Sony BMG Music Entertainment over its distribution of rootkit software. FTC Chairwoman **Deborah Platt Majoras** recently talked to Robert McMillan to discuss online advertisers' role in the adware and spyware.

CSO: Money is making its way to U.S.-based spyware vendors, hosting providers and advertisers. What can the FTC do?

Deborah Platt Majoras: I spoke [recently] to a corporate council. I told them that corporate America ought to do a better job of figuring out where their ad dollars are going. Because what we think is that some of the ad dollars are making their way to adware providers who may be providing the

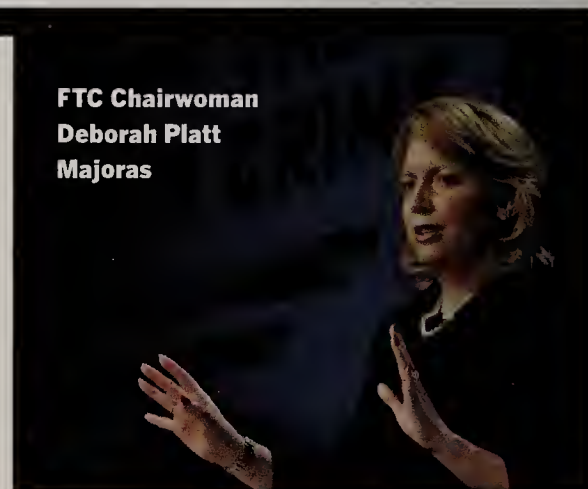
software without the consumer's knowledge and consent. And these companies may not even know about it.

If I were a company, I wouldn't think that having a consumer bombarded with pop-up ads advertising my product would be a great way to sell.

We want companies to have a better understanding of where these advertising dollars are going, so in a couple of our high-profile spyware cases, like the one against Zango [a \$3 million settlement], we tried to be very public.

You settled with Sony over its use of rootkit technology. Do you expect more conflicts between intellectual property and end users' rights?

It's not that [Sony] endeavored to protect



FTC Chairwoman
Deborah Platt
Majoras

their intellectual property, which they're entitled to do, it's that they didn't tell consumers what they were doing. We felt that how a consumer could use the CDs, where the music could be played ultimately, and whether or not their habits were being monitored, those were things that consumers would want to know about before they made their purchase. As we look at principles that we're applying in spyware and the like, the first principle is that the computer belongs to the user, not to the software distributor.

WHAT IF ALL CRIMINALS WORE PANTYHOSE OVER THEIR HEADS?



White-collar crime would be a cinch to spot. And businesses might not need easy integration of access control and video. They wouldn't care about smoothly transitioning to smart cards with the industry's first multi-technology reader. Wouldn't be interested in storing video with patented compression technology that uses less storage space and bandwidth. Wouldn't want their encrypted access control panel to be the most secure in the industry. If all criminals wore pantyhose over their heads, businesses wouldn't need our expertise to make security reliable and easy. Because it already would be. It all starts by completing the short questionnaire at www.tycoforyourworld.com or by calling 888-840-1438.

SECURITY FOR YOUR WORLD.



SOFTWARE HOUSE®

KANTECH

Access control and video systems

tyco / Fire & Security

the security **BLOTTER**

Breaches, scams and other recent incidents of note

DuPont scientist pleads guilty to stealing trade secrets. Gary Min pleaded guilty to one count of stealing trade secrets in a criminal case stemming from his agreeing to take a new job with a DuPont competitor in Asia. For almost two months before Min told DuPont he was leaving, he "accessed an unusually high volume" of documents from DuPont's electronic library of confidential information, according to prosecutors in the office of the U.S. Attorney for Delaware. The more than 38,000 files Min accessed related to the company's products and emerging technologies, and were worth an estimated \$400 million. Min faces a maximum of 10 years in prison, a fine up to \$250,000 and restitution.

TJX reveals data breach worse than originally reported. The retailer said on Feb. 21 that its ongoing investigation into a data breach showed its computer systems were compromised in 2005—about one year earlier than the company initially reported. The data accessed goes as far back as transactions recorded in January 2003 at stores in the United States, Britain and Ireland. As of press time, TJX had not disclosed how many consumers might be affected by the breach.

TV executive resigns after guerrilla marketing stunt ignites bomb scare. Jim Samples, executive VP and GM of the Cartoon Network, a unit of Turner Broadcasting, resigned nine days after emergency crews shut down parts of Boston on Jan. 31, *The Boston Globe* reported. The campaign placed 38 panels with blinking lights to advertise the animated show *Aqua Teen Hunger Force*. Turner agreed to pay \$2 million in restitution to the city.

How to Calm Someone in a Crisis

PASS IT ON Kelly Chessen was a suicide hotline counselor who later became a "data crisis counselor" at DriveSavers, which helps end-users recover their data and their composure. Share with colleagues in HR and management her list of tips for calming a distressed person.

1. Establish a rapport. A crisis state makes someone feel like no one can understand why he's upset, which in turn makes him more upset. To defeat this cycle, it's important to win the person's trust. Chessen uses a technique called validation. "Don't say, 'I understand,'" she says, because they won't believe you. "Instead, use indirect acknowledgement. 'I'd certainly be upset too.' Or, 'That must be frustrating. You have every right to be angry.'" Chessen adds that you should never tell someone in crisis how to feel, or say, "You need to calm down." Speak in a calm, even voice, which isn't always easy if someone is yelling at you. Chessen says she breathes deeply and speaks calmly even as she feels her temper rising.

2. Listen for signs of major problems. Chessen is alert for certain words and phrases that might indicate a person is in profound distress. "Sometimes I'll hear someone say, 'If I can't get my data back, I don't know what I'll do,' and that's a tip to me," she says, as are other statements such as "This is hopeless" or "My life is over." In every case, Chessen asks the person directly, "Are you considering suicide?" Whether it's a life event, or the loss of a critical work product at stake, it's crucial to ask. "If they're not thinking about it, they'll say no. And if they are, the fact that someone asked them to talk about it will be a relief and a release for them."

3. Give space and time. Let the person tell his story. Be an active listener, Chessen says,

which means "making sure the person knows you're part of the conversation by asking questions and injecting verbal cues, like 'Uh huh' and 'I see.'" Another technique is repeating to someone what they just said to you. "If they say 'I'm pissed my computer broke,' I say back, 'So you're upset that your computer failed. I'd be upset too.'" People feel better if they can tell their story, Chessen says.

4. Don't mislead the distressed person.

When Chessen is helping a DriveSavers caller, and she knows what's happening with equipment, she can reassure the person. "I can say, 'We can recover that kind of data 90 percent of the time,'" she says. It helps people in crisis to know the odds are on their side. But she also must acknowledge the 10 percent chance that the data won't be recovered. "If I don't, then I've broken that trust we've built up if that 10 percent chance actually comes true," she says. And that could prompt another crisis.

5. Develop an action plan. Once you have enough information, you can help the person in crisis explore his options, both in the current instance and for the future. It's important to avoid something that blames the person for what happened. (Don't say, "Next time, back up your data," for example.) What Chessen can do is have a portfolio of resources, such as backup products or services, plus information on how data is recovered from hard drives. Then it's time to build a plan for moving forward. The more concrete the plan—with tasks the person in crisis can do to ameliorate the situation—the better. Exploring alternatives and finding a path to a solution helps a person get through the short-term state of a crisis, Chessen says.

—Scott Berinato

SOURCE: "HOW TO CALM SOMEONE DOWN," WWW.CSOONLINE.COM/READ/120105/HT_CALM.HTML

It's OK to show off to your friends that you were in CSO.



But it's even better to show your customers.

What better way to inform your key customers of your editorial coverage in CSO than through customized Editorial Reprints?

Leverage the positive impact of your editorial coverage by using reprints for direct mail campaigns, seminar promotions, employee communications, recruiting and marketing

programs. Let us enhance your reprints with your company's logo, address, and sales message. Reprints make great SALES tools for trade shows, mailings or media kits.

And while a framed copy of your article will look neat on your wall, it will look even better in the hands of your customers.

CSO
The Resource for
Security Executives

PARS
Publishers
Ancillary
Revenue
Services
INTERNATIONAL CORP.
MANAGED REPRINT PROGRAMS

For more information on customized editorial reprints in volume quantities, contact:
Jennifer Eclipse at 212.221.9595 x237 or email jeclipse@parsintl.com.
Website: www.magreprints.com/quickquote.asp

Protecting the \$100 Laptop

The ultracheap computing device for developing nations presents unique security challenges

By Simson Garfinkel

THE \$100 LAPTOP designed for the children of the developing world poses one of today's most challenging sets of computer security problems. These laptops will be widely deployed to children who have no training in computer security, computer use or much of anything else, in some cases. They will belong to the children, go home with children and be customized by the children. And the laptops will provide Internet access using a new mesh network design that turns the laptops into wireless routers, allowing hundreds of children spread out across a village to share a single Internet connection.

Such a proposal would spell a security nightmare if these laptops were all running a stock copy of Windows, MacOS or even Linux. Hackers could steal a laptop, find a vulnerability and then write a worm to wirelessly hop from laptop to laptop, turning them all into the largest botnet that the world had ever seen.

Even worse, the One Laptop per Child project has enemies—from people who see \$100 laptops as a waste of resources when many communities don't even have clean water, to fundamentalists who are ideologically opposed to educating children with secular materials. Such enemies would almost certainly be motivated to create a piece of software to wipe the laptop's operating system and turn it into a \$100 brick.

Although botnets and bricks are a persistent fear of the laptop development team, the team is incorporating security measures into the design that are aimed at preventing both disasters from unfolding. Other security measures should reduce the incentives for thieves to steal the laptops, for parents to sell their children's laptops and even for kids to change their "From" address and get their classmates in trouble.

The \$100 laptop, officially called the XO-1 or Children's Machine, is a marvel of engineering, but it isn't a laptop that most adults would want to use. The laptop's keyboard is a small plastic membrane stretched over a circuit board:

It's resistant to water, and there are no moving parts, and it's definitely designed for children, not adults. The screen has a low-resolution color mode and a high-resolution black-and-white mode, in which it looks almost as good as paper but it's the size of a paperback book. The computer's CPU runs standard x86 instructions, but it's slow—only a few hundred megahertz. The machine has just 128MB of RAM, 512MB of main flash memory, 1MB of BIOS flash and no hard drive. There are also three USB ports, a Secure Digital slot, a microphone and a camera.

BIOS, to Boot

The BIOS flash is the laptop's primary defense against becoming a brick. As long as the BIOS is intact, the laptop can always boot from an external drive and have its operating system reinstalled. The BIOS also protects itself: It lives in write-protected memory that can be written only when the computer first boots. The BIOS will allow itself to be overwritten only with a new BIOS that is signed with four different digital signatures, the keys for which will be kept in a bank vault.

The XO laptop's operating system is a stripped-

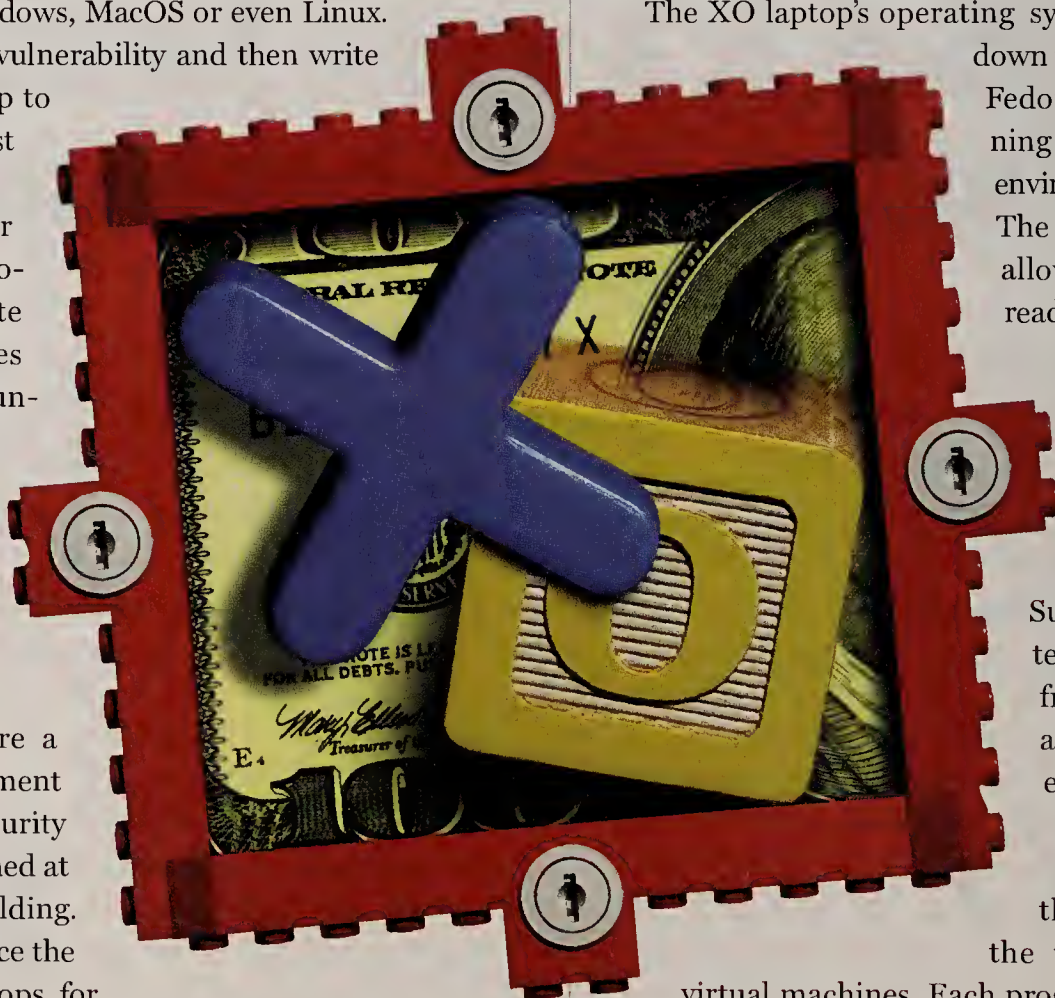
down version of Red Hat's Fedora Core Linux running a new user interface environment called Sugar. The goal of Sugar is to allow students to both read and create all kinds

of documents, to collaborate wirelessly, and even to write and share programs with one another. Yet

Sugar also has to protect a student's work from malicious code and allow students to easily recover from mistakes.

Sugar accomplishes this magic through the use of lightweight

virtual machines. Each program that a student might want to run (or write) operates in its own virtual machine that's isolated from the rest of the computer. The application has access to three directories—one for temporary files, one for configuration information and one for data. This gives a game a



reasonable place to store its high-score file. The rest of the computer's file system is invisible.

Of course, there are many kinds of data that should be shared between applications—like photographs, movies and word processor files. Sugar stores such documents in a special set of directories managed by an application called the Journal. The Journal automatically indexes its information by media type, contents and the date that it was created or modified. The idea is to free children from having to be file clerks—something that even adults don't do particularly well. (Ever see the desktop of a Windows or Mac computer littered with several hundred icons?)

When students wish to work with an image or on an essay, they'll pick the data inside the Journal. The Journal will then open the file and hand a reference to the opened file to the activity. An application can also instruct the Journal to ask the user to choose an object—for example, to specify a photo that might be included in a word processor document. Once again, the Journal returns to the application a reference to the opened file—the application never gets to run the open system call itself. This prevents a variety of attacks that are endemic on PCs today—for example, the malicious screen saver that surreptitiously opens and edits the contents of your word processing files.

Despite its strengths, the XO's radical hardware design opens up the potential for some new kinds of attacks—attacks that need to be prevented before the laptop can be deployed.

Consider the XO's flash storage. Unlike conventional RAM or hard drives, flash memory is limited as to the total number of times that it can be erased and rewritten. A malicious program could try to break the XO's flash by repeatedly rewriting the contents of one or more files until that lifetime has been exhausted. To prevent this kind of attack, every running activity on the computer is given a quota for how many sectors it can erase and rewrite per minute. Activities that use up their quota get slowed down and

eventually suspended until their quota is replenished.

Another potential attack is made possible through the XO's microphone and videocamera. A hostile program could turn these on and use them to eavesdrop on a child—or that child's family. Such attacks have already happened in the

The current plan is for each laptop to create its own digital certificate when it is activated by its student owner.

United States, with literal spyware turning on desktop webcams and transmitting the images to nefarious voyeurs. The XO's designers have addressed this potential problem with two bright LEDs mounted next to the videocamera: One LED turns on whenever the microphone is energized, the other alerts that the videocamera is in use.

Antitheft Measures

Theft is a serious problem in many of the countries where the laptop is sure to be deployed. Although the XO's child-size keyboard, tiny screen and bright green color should hopefully be theft deterrents, One Laptop Per Child has also designed an antitheft system that the countries purchasing the laptop can choose to enable and operate.

The antitheft system works a lot like Microsoft's Windows Update or the Activation feature that's built into Windows Vista. Each laptop has a unique serial number that's assigned when the laptop is created. Every day the laptop tries to make a connection over the Internet to a centralized server run by the customer (that is, by the country or education system, or whoever bought the laptops). Once the

connection is made, the XO reports on its health and checks for updates. If updates are available, they are automatically downloaded, checked for a valid digital signature and then installed.

Laptops that are reported stolen are given a special update that causes the laptop to disable itself until it is returned to the school where its owner is registered—and from where the original theft report was filed. If the laptop is never returned, it will never work again. If the laptop is returned, it can be reactivated. Laptops can also be configured to automatically disable themselves if they haven't been able to reach the update server for a predetermined period of time—say, one or two weeks.

One area where the laptop's security approach will be very different from Microsoft's, however, is identity management. The current plan is for each laptop to create its own digital certificate when it is activated by its student owner. That certificate might contain the student's first name, photograph and other information—but it won't be digitally signed by the school, the ministry of education or anyone else. So these certificates could be used to sign chat and e-mail messages (so that students can't forge messages from one another), but they won't work as the basis of a national electronic identity system.

If these security measures seem familiar, they should: Many of them have been taken from other systems currently in the field or being tested in the lab. But the XO is the first system that puts them all together, and the first example of a computer maker trading compatibility with legacy applications in favor of strong security. If the XO is successful, my guess is that many computer users might be interested in making a similar trade for themselves. Expect to see these ideas showing up not just in Linux, but on MacOS and even Windows in coming years. ■

Simson Garfinkel, CISSP, is researching computer forensics and human thought at Harvard University. Send feedback to machineshop@cxo.com.

More than just another data-security standard, **the PCI program** is corporate America's most ambitious effort yet to prove that it can self-regulate. But even a standard with everything going for it might not be enough to stop the loss of credit card data. **By Sarah D. Scalet**

IN MID-DECEMBER 2006, just as Visa was announcing a \$20 million incentive to try to hurry compliance with the credit card industry's data-security standard, a consultant for TJX was discovering precisely the sort of breach that the standard is supposed to prevent.

An undisclosed number of transaction records from TJ Maxx, Marshalls and other TJX stores had been compromised. "Removed" by intruders, even. Exactly which records, when and by whom, the \$16 billion retailer was unsure, although *The Wall Street Journal* later put the number of affected credit cards at more than 40 million. Behind the scenes, TJX executives began working with law enforcement and additional outside security experts to try to identify and fix the problem, prior to a January announcement of the breach.

Meanwhile, in San Francisco, Visa was going public with an announcement of its own. Technically, if its merchants aren't compliant with the Payment Card Industry (PCI) Data Security Standard, Visa can cut off their ability to accept Visa cards—a death sentence for commerce. Despite deadlines that had come and gone, however, only 36 percent of Visa's largest merchants were following the rules. So starting in April, banks whose retail customers were in compliance and had not suffered security breaches would be eligible to receive funds from a pool of up to \$20 million. In addition, Visa warned, it would increase fines to banks whose retail customers were not compliant and make PCI

IN THIS STORY What the PCI standard is supposed to do ■ Why compliance is going slowly ■ How that might affect industries' future attempts to self-regulate

Standardized Tests



**Royal Ahold Global
Information Security
Officer JOHN KIRKWOOD
says a PCI audit for one
card association doesn't
always satisfy the others.**

certification a requirement for some pricing discounts.

As far as Visa is concerned, the standard is working—if only merchants would adopt it. “To date we have not seen that a PCI-compliant entity has been compromised,” Eduardo Perez, vice president for payment system risk at Visa, told CSO in January. Although he would not comment on the TJX incident specifically, he continued: “In every instance we’ve dealt with, compromised entities have not been compliant with PCI.”

For critics, however, the TJX breach proves something else entirely. “It’s a perfect example of where the PCI program is not working,” says Avivah Litan, vice president and research director at Gartner. “It’s a good step. It’s good for the card brands to enforce security, but it’s impractical to expect 5 million retailers to become security experts.”

In reality, the TJX breach is not so much an example as it is a test. Corporate America has long insisted that self-regulation, not government intervention, is the cure for what ails information security. Government regulations, they claim, tend to be poorly crafted and difficult to enforce; they turn into needlessly expensive exercises in bureaucratic paperwork. In response to the threat of such legislation, industry sectors have attempted to police themselves by establishing either voluntary guidelines or ones imposed by business partners. (See “Power Play,” www.csoonline.com/010107.)

The PCI program is the largest, most ambitious of such efforts to date. Last autumn, American Express, MasterCard, Visa and other highly competitive rivals came together to fund an independent PCI Security Standards Council, which will promote and drive a single data-security standard. In the midst of a steady stream of credit card breach announcements from companies large and small, the message the card associations wanted to send was clear: They are doing something about the problem.

But will it be enough?

“Remember, the reason the PCI standard exists is to avoid legislation from Congress,” longtime CISO John Kirkwood says plainly. Kirkwood is no stranger to PCI. The former CISO of American Express, he is now global information security officer for \$52 billion Dutch grocery-store chain Royal Ahold, where he has to make sure that subsidiaries such as Stop & Shop comply with the standard. He has dealt with his own recent security breach, involving checkout equipment tampering in at least six Stop & Shop stores in Rhode Island and Massachusetts.

“The credit card companies said, hey, wait a second, you don’t have to legislate us. We’ll regulate ourselves,” Kirkwood continues. “It’s going to be very interesting to see what happens in light of the TJX incident. I can see another [Gramm-Leach-Bliley Act], another Sarbanes-Oxley coming.” Indeed, soon after the breach was disclosed, as TJX-related cases of fraud started to surface, legislators began pointing to the incident as further proof that Congress must take action.

All of which means that it’s showdown time in the battle between government regulation and preemptive industry self-regulation. Businesses that accept, process and enable credit card transac-

tions will have to convince legislators (not to mention the American public) that the PCI program is going to prevent data breaches. If they can’t, the implications will reach far beyond the payment card industry, as the PCI standard goes down in history as nothing more than a crash test of private industry’s ability—even under the best possible circumstances—to regulate itself.

A Sharp Stick

The roots of the PCI standard date back to the summer of 2000, when Visa unveiled its “Digital Dozen” of rules that merchants needed to follow in order to accept its credit and debit cards. The requirements ranged from installing firewalls to encrypting data to restricting physical access to cardholder information. “Eventually, if we don’t have proof from an independent third party that you qualify with our requirements, we really don’t want you to take the card,” a Visa executive told *CIO* magazine (a sister publication to *CSO*) in 2002.

Visa, it was clear, had an especially pointy stick with which to prod its business partners—and, with its cards accepted at millions of locations worldwide, an especially far-reaching group of business partners who could be prodded. American Express, Discover and MasterCard soon whittled similar sticks to prod far-reaching business partners of their own. Compared with, say, the federal government’s ineffectual attempts to enforce the Health Insurance Portability and Accountability Act, card companies’ chances of success seemed promising. They had both resources and commercial clout. “Ultimately the reason companies need to be able to comply with PCI is that Visa and MasterCard have the ability to cut them off,” says Mark Rasch, a former federal prosecutor who’s now a computer security consultant. “You could pay a fine. If you’re a large financial company, you could pay a fine of a million dollars. But if they told you tomorrow that you can’t process credit cards, you’re out of business.”

Not surprisingly, though, merchants balked. As the standards from the various card associations grew and took shape, merchants had two main complaints: first, that there were too many standards, and second, that they had insufficient input into how standards were formed.

“Merchants had to certify with each brand,” explains Julie Ferguson, cofounder and board member of the Merchant Risk Council, a trade association. “Each of the four were coming up with their own individual products and weren’t necessarily talking to one another.”

To address these concerns, more than half a decade after Visa’s Digital Dozen was created, rival card companies came together to form an army of sorts. The PCI Security Standards Council was created last September as a joint agreement between American Express, Discover, JCB, MasterCard Worldwide and Visa Interna-



PCI Data Security Standard
The standard for protecting
cardholder data.

tional. Each of the companies contributed seed money and agreed to push jointly for a single set of security requirements—this being the PCI Data Security Standard, which still has 12 main criteria that encompass installing firewalls, encrypting data and restricting physical access to cardholder information, among other things. A primary goal of the common standard is to prevent merchants from ever storing all the data on a card's magnetic strip, which may contain private cardholder information as well as PINs and the printed security codes that help merchants authenticate online transactions. (See "PCI To-Do List" on Page 20 for highlights of the standard.)

With the creation of the council, all suggestions and changes to the rule book are now funneled through this group. Furthermore, the council determines which auditors are qualified to perform PCI

assessments and which vendors are qualified to perform scans for vulnerabilities or misconfigurations in an organization's infrastructure. Eventually, says chairwoman Seana Pitt, the council's funding will come not from the card associations but from training and certification fees.

"What we're evolving to is becoming a center of excellence," says Pitt, who is also a vice president at American Express. "Anybody who has questions about interpreting the standard or suggestions on making it better will come to us, whereas in the past they would talk to the individual brands."

The sticks, meanwhile, stay in the hands of the individual card associations. That's because the standards council itself has no enforcement capability. In fact, when asked in January about current compliance levels, Pitt admitted that the council has no numbers to benchmark against. Instead, members will measure their success based only on feedback from the card companies and members.

"We actually get the happy part of driving education and compliance," Pitt says. "Or the proactive part," she clarifies.

The Technicalities

At Marriott International, Chris Zoladz is among those who are working to comply with the PCI standard. The \$12 billion hotel chain has been working on the standard over the past few years, but "it's quite an undertaking to get to the point of full compliance," says Zoladz, who is Marriott's vice president of information protection and privacy.

One pain point is the encryption requirement. Although Marriott has long been encrypting data while it's in transmission, the PCI standard also requires that data be encrypted at rest, something Marriott had not been doing because other protections were in place. Card data is initially saved in a central reservation system but later gets passed on to a property management system for the individual hotel where the customer has booked a room. The challenge, Zoladz says, is to encrypt the data as it is stored in both places while still allowing the systems to talk to one another.

Another pain point is the requirement for two-factor authentication. The standard stipulates that a user name and password are not enough to authenticate an employee, administrator or third party who gains remote access to any system that holds debit or credit card data. In addition, the merchant must set up a second factor of authentication, such as tokens or biometrics. That's no



PCI To-Do List

Highlights of the 17-page Payment Card Industry Data Security Standard

small undertaking for a company with a large, dispersed workforce like Marriott's.

Not that Zoladz is complaining about the changes, mind you. "I think the standard is pretty solid," he says. "When I look at each of the requirements in the standard, a lot of what's in there is very consistent with what you find in the ISO 17799 standard or what you would find in any of the various articles and publications around best practices in information security."

Likewise, at CheckFree, Vice President and CSO Ed Sarama is still working on his company's PCI compliance. "Nothing is easy in the IT world," says Sarama, whose \$880 million company does payment processing for many of the United States's largest banks. "We like for everything from a consumer perspective to be magical, but there's a lot of work behind the scenes, and this is no exception."

Sarama says the main challenge he's having is that the standard is a moving target. For instance, last autumn, the PCI Security Standards Council made some changes to retention requirements that affected CheckFree. Now, an audit trail of all access to cardholder data and network resources must be available online for three months and offline for another nine months, which means that CheckFree has to invest in additional online storage devices. Another change means that CheckFree must put application firewalls in front of its Web servers; Sarama has to figure out how to do this in a way that won't cause any applications to fail.

On any given point, the fallback to meeting the letter of the law is meeting the spirit of the law. In PCI-land, this is known as a "compensating control." Ken Rowe, a principal of the consultancy Chief Security Officers, and a certified PCI assessor, knows all about compensating controls. For instance, he's working with one city government whose network isn't segmented with firewalls, as the PCI standard requires. That means that the entire network must be in compliance with the standard—not just the portions of it, such as the ticketing application for the performing arts center, that actually house card data.

"There are other compensating controls in place, like VLANs and access control, that prevent someone from another department accessing credit card numbers," Rowe says. "But the standard calls for segmentation using firewalls," so that's what the city government is working on.

BUILD AND MAINTAIN A SECURE NETWORK

REQUIREMENT 1: Install and maintain a firewall configuration to protect cardholder data.

REQUIREMENT 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

PROTECT CARDHOLDER DATA

REQUIREMENT 3: Protect stored cardholder data.

REQUIREMENT 4: Encrypt transmission of cardholder data across open, public networks.

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

REQUIREMENT 5: Use and regularly update antivirus software.

REQUIREMENT 6: Develop and maintain secure systems and applications.

IMPLEMENT STRONG ACCESS CONTROL MEASURES

REQUIREMENT 7: Restrict access to cardholder data by business need to know.

REQUIREMENT 8: Assign a unique ID to each person with computer access.

REQUIREMENT 9: Restrict physical access to cardholder data.

REGULARLY MONITOR AND TEST NETWORKS

REQUIREMENT 10: Track and monitor all access to network resources and cardholder data.

REQUIREMENT 11: Regularly test security systems and processes.

MAINTAIN AN INFORMATION SECURITY POLICY

REQUIREMENT 12: Maintain a policy that addresses information security.

VERSION 1.1, RELEASED IN SEPTEMBER 2006

Some of the technical issues may work themselves out sooner rather than later. For instance, at PayPal, CISO Michael Barrett—another American Express alum—is trying to figure out what to do about the standard's vague stance on whether Unix servers must have antivirus software installed.

"PCI says this [need for antivirus control] is more applicable if you're running Windows servers and less applicable if you're running Unix servers," says Barrett, whose company, an eBay division, processed \$37.8 billion online payments during 2006. "It doesn't actually say, if you're running a Unix server you're exempt from the requirement. You get into discussions with auditors about whether it's enough. I expect PCI to mature over the next year or so, so that those discussions become much more routine."

Likewise, the vulnerability that Stop & Shop dealt with, involving criminals who tampered with the equipment customers use to swipe their credit cards and input PINs, is not currently addressed in the PCI standard. "I think the standard will mature," Kirkwood says, "and as it matures, it will be more comprehensive." (For details, see "Bolting on Security at Stop & Shop" at CSOonline.com.)

The bigger issue for CSOs, however, may be the nature of the discussions with the standards council, and how united a front the credit card associations are really presenting.

Barrett and Kirkwood both mention that a PCI audit acceptable to one card association does not always satisfy the other associations. Kirkwood says, "It's the same standard, but it's not like you can say you're PCI-compliant and then you're done for all the entities. Why don't we have one PCI assessment of Ahold, and have that apply to everyone? I think that's the way we're going to evolve; we're just not there yet." Kirkwood thinks he understands the reasons

why. "At American Express, we couldn't rely on Visa certification, because if something happens to the merchant, then American Express would be in a really bad situation, saying they relied on what Visa did. The public would say, why did you do that?"

Council or no, Kirkwood says, it's simply hard for any one body to take on that kind of responsibility. "If a central organization says, 'We certify ChoicePoint,' who gets sued when ChoicePoint has a problem? If you did that, you would have to have a limitation of liability that says something like, 'We'll review them, but don't hold us accountable if something happens to them.' Therefore the

certification doesn't mean too much."

Suddenly, government intervention doesn't sound like such a crazy idea.

The Best of All Possible Standards?

Of course, there are a raft of reasons why government intervention doesn't work much better than the PCI standard. Look no further than HIPAA, which contains both security and privacy provisions for healthcare organizations. Despite the fact that the law is more than a decade old, there have been no fines to speak of, leaving some organizations scratching their heads about why they should bother complying. Meanwhile, federal CIOs and CISOs complain that the 2002 Federal Information Security Management Act has turned into nothing but an exercise in completing paperwork, rather than improving security. The one piece of federal legislation that did prompt widespread work on information security controls—the Sarbanes-Oxley Act—stemmed from one small section, 404, and corporate America is currently in rebellion that the end has not justified the multimillion-dollar means. The problem is always an economic one—not that compliance costs too much money, precisely, but that the money it costs isn't worth spending.

The challenge for the card associations now is twofold: to prove the value of the PCI standard in and of itself, and to create an incentive system that gives organizations the final shove if the standard on its own doesn't provide enough value. One-time compliance incentives may simply be too small. Visa's \$20 million incentive could be split up by as many as 33 merchant banks, which could then choose (or not choose) to pass on the incentives to thousands of their merchant customers. And even fines may not be enough. Visa, for instance, levied \$3.4 million in fines in 2005 and \$4.6 million in fines in 2006. But compliance likely would have cost fined organizations even more.

"It's kind of like, you can drive a car without car insurance, but if something happens you're going to be in big trouble," says Rowe, of Chief Security Officers. "I think a lot of [merchants] are accepting the risk and hoping the controls they have in place will prevent a breach even though they may not be in compliance."

The associations, leery of exercising their death penalty, have done so only once. After hackers accessed some 40 million card numbers stored by payment processor CardSystems Solution in 2005, both Visa and American Express cut off the company's ability to process payments. The company went into bankruptcy, where its assets were acquired by Pay By Touch. CardSystems disappeared.

More encouragingly, Visa has announced that it will start making PCI compliance a requirement for some reductions in the

interchange fees they charge to merchants who accept credit card payments. This is more a backward penalty than a new incentive: A merchant that currently qualifies for the reduced fee, known as tiered interchange, could lose that reduction because it's not PCI-compliant. Visa's Perez says the largest merchants could stand to lose millions of dollars annually. "It's a very compelling incentive," he says.

Count on chief security officers—risk managers at heart—to look at all these changes pragmatically. "If I was going to get fined \$5 million but I brought in \$150 million in business, that's fine," Kirkwood says, speaking hypothetically. "It becomes a cost of doing business." A bigger motivator, however, is interchange fees. "That impacts the profit per transaction, which has a much bigger potential than anything else."

Since announcing the changes, Visa has seen some increase in

its compliance rates. Among what are known as Level 1 merchants, which process more than 6 million Visa transactions per year, compliance rose from 36 percent in December 2006 to 40 percent in January 2007. Among Level 2 merchants, which process between 1 million and 6 million Visa transactions each year, compliance inched up to 16 percent from 15 percent since the Level 2 requirements took effect in July 2006.

In the same time period, however, calls for regulatory action stepped up even more quickly. Shortly after the

TJX breach disclosure, Barney Frank, chairman of the House Financial Services Committee, issued a stern rebuke, calling the incident "further evidence" of Congress's need to intervene. "[T]hose institutions where breaches have occurred must be identified and they must bear responsibility," the Massachusetts Democrat said in a statement. "Specifically, this means retailers or wholesalers must take responsibility, contrary to what common practice is today."

No one really wants more regulation; everyone just wants the security breaches to stop. Jay White, global information protection architect at Chevron, where some business units must comply with the PCI standard, isn't alone in pointing out that it would, in theory, be easier for private industry to police itself. "There are times when you are applying resources just for government compliance as opposed to having it add any business value," White says. "I would rather have industry be self-regulated, until companies demonstrate that they can't self-regulate."

The PCI standard is corporate America's big chance to demonstrate that it *can* self-regulate. The question now is, How long before it will have proven just the opposite? ■

"I would rather have industry be self-regulated, until companies demonstrate that they can't self-regulate."

—JAY WHITE, CHEVRON

Reach Senior Editor Sarah D. Scalet at sscalet@cxo.com.

THE SCOURGE OF Image SPAM

How the latest iteration of junk mail is beating filters and filling inboxes

BY SCOTT BERINATO



MAGE SPAM—an e-mail solicitation that uses graphical images of text to avoid filters—is not new. Recently, though, it reached an unprecedented level of sophistication and took off. A year ago, fewer than five out of 100 e-mails were image spam, according to Doug Bowers of Symantec. Today, up to 40 percent are. Meanwhile, image spam is the reason spam traffic overall doubled in 2006, according to antispam company Borderware. It is expected to keep rising.

The conceit behind image spam is graceful in its simplicity: Computers can't see.

All spam-thwarting techniques rely heavily on filters—programs that inspect words, phrases, mailing histories, IP addresses, shapes and other aspects of an e-mail. Those filters have lists, or dictionaries, of things that make any given

message “spammy.” If a message seems spammy enough, the filter blocks it.

The spammer's challenge, then, is to deliver something that the filter hasn't yet learned is spam. Eventually, the filter incorporates the new derivations into its list of spammy traits. Then the spammer changes convention again, and on and on. Thus *Viagra!* becomes *V1agr@!* becomes *V”iA’g R@!* and so forth.

But even as they block more messages, spam filters don't get smarter as much as they get stronger. Their dictionaries of unacceptable traits grow, their IP blacklists get longer, and the processors that power them get more horses. But for the most part, filters don't change what they do even if they can do more of it. However complex or strong, they still just parse text and HTML looking for spam.

Parsing an image, on the other hand, ain't so easy. There's so much data in an image that a filter sees noise—millions

of 0s and 1s in no discrete pattern. Yet the human eye and brain, in a fraction of a second, intuit from the same image, *That's Viagra!*

Spammers have made image spam really effective by using not just one but multiple filter-thwarting techniques. Some confuse optical character recognition filters, some automatically alter images to create randomness, and some even buffer against defenses that don't yet exist but that spammers anticipate will be built in response to image spam. Couple all that with the fact that a single image spam message, on average, is more than twice the size of an HTML or text-based spam, consuming all kinds of bandwidth and storage on networks, and you have a scourge.

But to battle it, first you must understand it. Turn the page to learn all the ways image spam is beating filters and clogging networks with useless e-mail.



The CSO Executive Seminar Series on

PRIVACY

CHICAGO, ILLINOIS

May 17, 2007

Hyatt Regency McCormick Place

Register today at www.csoonline.com/conferences.

The CSO Executive Seminar Series on Privacy will provide attendees with an oversight briefing on personal data and identity theft liabilities, as well as privacy issues for executives in both the government and private sectors. This program will examine the overarching issues, the players, the legal issues, the options available and damage control when something goes wrong.

WHO SHOULD ATTEND

CSOs, CPOs, CISOs, Security & Privacy Protection Managers, Legal Counsels and others who are charged with preparing for privacy breaches.

Government and non-profit officials who prepare their organizations for security issues.

BENEFITS OF ATTENDING

A 360 degree view of identity management including:

- Key identity management implementations
- Building a business case for identity management
- Navigating the roadblocks to success

Visit www.csoonline.com/conferences to view the entire agenda.

Space is limited. Register today at www.csoonline.com/conferences or for more information call 800.366.0246.

Produced by:

CSO
The Resource
for Security
Executives

Image SP-AM

By the Numbers

1

ATTENTION! WATCH VGYI.PK ON 25 SEPTEMBER, MONDAY!

Last week, massive interest was on VGYI.PK, which more than doubled the price.

VISION ENERGY GROUP NEW (Other OTC: VGYI.PK)

Current Price: \$0.75

Expected: Heavy Price Increase for Monday, SEPT. 25th

BREAKING NEWS!

LOS ANGELES--(BUSINESS WIRE)--Sept. 18, 2006--Vision Energy Group (Pink Sheets: VGYI - News) now wishes to advise that an agreement has been completed and signed with Valley Production Inc., the Oil & Gas Production Group from Bakerfield, Calif., to jointly process low quality natural gas from two existing wells.

About Vision Energy Group

Vision Energy Group offers several renewable and alternative energy technologies and know-how and is working toward putting these designs into practice in commercial production.

The company has noted a high volume of share sales on 9/18/06 and would recommend that shareholders consult their Brokers or advisors before taking any action.

Investors Are excited As "Hound Dog" Continues to make the news! More news expected Thursday!

4

The Motion Picture Group
Symbol: MPRG
Price: \$0.22

Investors are excited As "Hound Dog" Continues to make the news! More news expected Thursday!

Investor ALERT! MPRG Secures \$10 Million for New Film!

The Motion Picture Group
Symbol: MPRG
Price: \$0.22

MPRG secures 10 Million to fund a film from the Co-Author of "How To Lose A Guy In Ten Days". The New film "April In December" is set to begin filming in 2007 and is labeled as a Romantic Comedy. This is gonna rock this stock on Friday. Read the news and get on board for a BIG cash ride with MPRG.

2

Last week massive

3

Last week massive

Last week massive

From: bromide [baselconsanguineous@prost-partner.de]
To: branko@borderware.com
Cc:
Subject: Pick it as early as possible
Sent: Mon 9/25/2006 7:47 AM

ATTENTION! WATCH VGYI.PK ON 25 SEPTEMBER, MONDAY!

Last week massive interest was on VGYI.PK, which more than doubled the price.

VISION ENERGY GR NEW (Other OTC: VGYI.PK)

Current Price: \$0.75

Expected: Heavy Price Increase for Monday, SEPT. 25th

BREAKING NEWS!

LOS ANGELES--(BUSINESS WIRE)--Sept. 18, 2006--Vision Energy Group (Pink Sheets: VGYI - News) now wishes to advise that an agreement has been completed and signed with Valley Production Inc., the Oil & Gas Production Group from Bakerfield, Calif., to jointly process low quality natural gas from two existing wells.

About Vision Energy Group

Vision Energy Group offers several renewable and alternative energy technologies and know-how and is working toward putting these designs into practice in commercial production.

The company has noted a high volume of share sales on 9/18/06 and would recommend that shareholders consult their Brokers or advisors before taking any action.

Please don't click. Enter manually following address in address bar of your browser: **www.dvarx.com**

about:blank - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address www.dvarx.com Go

Just type
www.dvarx.com
in address bar
of your browser

8

This is the second reported killing by stray dogs in the same neighbourhood in less than two months. It said that headline Hindu organisations had planned the riots months before they occurred

7

6

5

9

Image Spam Techniques

1 GIF Layering

Just as word splitting divides words into multiple images to elude spam filters (see number three), an image spam can be divided into multiple images. Like the transparent plastic overlays in *Gray's Anatomy*, pieces of a message are layered to create a complete, legible message. In this rudimentary example, the spam is divided into three pieces (cut in the middle of letters for added obfuscation). But one message could comprise as many as a dozen layered GIFs.

2 Optical Character Recognition Duping

Optical character recognition (OCR) is the closest to sight that computers get. OCR works by measuring the geometry in images, searching for shapes that match the shapes of letters, then translating a matched geometric shape into real text. To defeat OCR, spammers upset the geometry of letters

enough—by altering colors, for example—so that OCR can't "see" a letter even as the human eye easily recognizes it. The effect is something like blurred characters in an eye test.

3 Word Splitting and Ransom Notes

If OCR catches up to the color tricks in image spam, a spammer's next defense is word splitting. By dividing the image and leaving space in between the pieces, any image the OCR engine is examining is only a piece of a letter with its own distinct geometry. Instead of word splitting, some spammers have employed a ransom note technique in which each letter in the spam message is its own image, and each letter image includes background noise and other baffling techniques. A program cobbles together randomized letter images to make words. The effect looks like a classic ransom note with a mishmash of letters cut out from magazines.

4 Geometric Variance

Many filters can intercept mailings based on their sameness. Images, though, can be altered easily without disturbing the message inside them. Thus one spam message will arrive as dozens of differently shaped images, and each time the colors of the text images will have changed, as will the randomly generated speckling and pixel and word salads. No two images are alike despite the fact that they carry similar messages. Shown are two radically different images containing the same stock tip. The technique is popular as a scheme to boost prices of low-value stocks. In March, the SEC suspended trading on 35 such stocks that were the subject of these image spam messages, including some whose prices rose.

5 Speckling

Confetti-like speckles don't affect the legibility of the necessary information but make every message unique to confuse a filter looking for patterns or high volumes of identical images.

6 Pixel Salad

A bar of randomly generated color pixels contains the vast majority of the image data. To a filter it's full of patternless noise. We can see the words in the message while the image at the bottom doesn't bother us.

7 Hyperlink Elimination

Many image spam messages lack hyperlinks because filters have improved their ability to find and trace spammy URLs and then block the message based on the inclusion of a bad link. To get around this, spammers will ask recipients to type the URL into their browsers.

8 Word Salad

A classic element of spam, word salads are text passages, often taken from novels like Jane Austen's *Pride and Prejudice*, designed to confuse Bayesian filters and weighted dictionaries. A Bayesian filter uses complex math to determine the probability that some combination of words is spam. Weighted dictionaries score the words in an e-mail depending on how

spammy those words are. If an e-mail scores above a certain threshold, it's flagged. The words in a word salad don't score as spam, so they pull the overall score below the threshold. The filter sees predominantly natural text it can't flag as illegitimate. Word salad also offsets filters that by default block e-mails that are devoid of body text and contain only a GIF image.

9 Animated GIF If you program a GIF to overlay its layers slowly, you end up with an animated GIF, which has a similar effect as GIF layering. It's sort of like a flip book. Here, with www.dvarx.com, each letter is a GIF layer. As they are piled on top of each other, it looks to the eye like someone typing in the letters into the address bar.

From Plain Text to Image Spam

How the word Viagra has stayed ahead of spam filters through the years

Viagra! A simple text message	V1agra! One character exchanged to dupe text filters	Via<!--hi-->gra HTML comments are invisible to user but fool filter	V1agr@! Multiple characters exchanged with symbols	Vi<asdf>ag<asdf>ra Bad HTML is invisible to user but confuses filter	V' 1ag^r"a Complex character disguising	Vi ag ra Good HTML breaks up word to appear: Vi ag ra
---	--	---	--	--	---	--

VIAGRA





The Scoop on Loss Prevention

Friendly's Restaurants' Ernie Patnode approaches cash management with a lot of common sense, a little technology and, yes, politeness By Scott Berinato

erne Patnode likes to say that cash handling is a lot like passing sand from hand to hand. The more hands involved in the process, the less sand you'll have left at the end.

Patnode is corporate security manager for Friendly's Restaurants, an ice cream and burger joint familiar to any New Englander. And part of Patnode's approach to loss prevention in his company's 510 restaurants (some owned, some franchised) is to minimize the number of hands passing the sand. "It's basically about honesty," says Patnode. "There's no magic about it." But Patnode's philosophy is broader than that, and parts of it are surprising. Loss prevention programs are often tagged as "gotcha" operations, a policing function that doesn't contribute to the business unless it's stopping someone from skimming the till. But Patnode, who retired from the Massachusetts State Police 18 years ago and who has been with Friendly's ever since, doesn't

adhere to that philosophy. Underlying his loss prevention program, which he believes can enable the business, is significant respect for

human nature, even empathy for someone trying to buck the system. He approaches loss prevention with a healthy dose of niceness, saying that all those tools used to catch bad guys in the act of stealing ought to be used as much for rewarding good guys with praise.

CSO spoke with Patnode about his approach to effective cash handling and loss prevention.

CSO: Which comes first in your loss prevention program, technology or policy?

Ernie Patnode: In many ways, your policy and sticking to it, that's more important than technology when it comes to loss prevention. If you have a good policy and are strict about enforcing it, that's key. For example, you can install various types of cards and all that, but you know what? A waiter leaves his access card unattended, something still happens. It's a policy violation that got you. Electronics are trackers. It's the same as card access to headquarters' offices. It tells you who entered, what time, how long the safe door was open. It helps tracking supervisory staff. But it isn't like you have something that reads every single action. The strength of most loss prevention is good solid supervision. Look, systems are great, don't get me wrong, but loss prevention comes down to having top-notch supervisory staff.

IN THIS STORY CCTV catches employees doing right ■ Building design as a security tool ■ Dealing with armed robbery

Loss Prevention



Still, technology must be important. What do you focus on?

I'm a firm believer in CCTV and alarm systems. Our back doors are locked with alarms when possible. Pass doors, where trucks drive right up and deliver goods right into the freezer, we put monitors on those to record entry and trigger CCTV, and also alarm if someone walks out without having already walked in. The CCTV, we've done studies on the new stuff. Things like being able to bring it up on my office PC. It's a substantial financial investment we weren't ready to make. So what we did do is invest in cameras that allow for the upgrade if we decide we need it. I want to research its value more.

Vendors always say [a product] can do X, Y and Z. But to me it's just as important to use these tools to prove someone's innocence as it is to prove someone's guilt. People look at the technology as a means to deterrence and penalty. It's not bad bad all the time. I look at it as an opportunity to reward people for doing the right thing. Rewarding someone makes them a better employee who is less likely to steal.

Using CCTV for praise. That's a new one.

Praise is important. Thanks. Acknowledgment. It makes you become part of the institution, part of the team when you're praised. And guess what? Now I've got an extra pair of eyes and ears in the restaurant. After this [interview], I'm going to stop at a couple of restaurants. Drop in. See what's going on. Tell those guys some of the good things I see.

It almost sounds like intelligence gathering, in a benign sort of way.

Who knows what's really going on better than the supervisors in the field? Not a camera or a computer.

What's something people misunderstand about loss prevention?

In the restaurant industry, one of the things about loss prevention is that it goes way beyond money. It's not always cash. It's food. Inventory. Nowadays we run reports on what was shipped to each res-

Know Your Loss Prevention Terms

Bleeding: Removing money from registers and depositing it in a safe. Used to prevent too much cash from sitting out in tills.

Bleed boxes: Lock boxes used to transfer money from till to safe. Used to secure the money from supervisors who do bleeding.

Waitstaff banking: Using waitstaff to settle bills, as opposed to host/hostess banking, whereby bills are settled by one person up front. Each method has its benefits and drawbacks from a loss prevention standpoint.

Excessive couponing: Fraud technique in which waitstaff or host collects coupons from newspapers and then rings them into orders without customer's knowledge, pocketing the difference.

Excessive discounting: Fraud technique in which waitstaff or host applies discounts on meals (ringing in a senior citizen discount on what should be a full-priced order, for example) and pockets the difference.

Dual custody: The use of two individuals to independently handle and count cash for accountability purposes.

taurant and what was used, every day. We should be able to match inventory to sales. If inventory comes out too low, it's a loss. But what if it comes out too high? Too much inventory is just as much a problem. Some managers get bonuses for efficiency, and they could be padding the inventory to receive their bonus. That's larceny.

Or, if an employee eats and fails to pay for the meal, that's a loss. Even if they say it was a mistake, it still costs the restaurant money. We can't eat mistakes, so we let them know it has to be reconciled. Ring it in when you eat. Instill in the cooks that if you prepare a meal and there's no receipt for it, you are partly responsible for the loss.

But, come on, it's just a burger for a hard-working teenager.

Say you sell a product—a meal—for \$10.

The employee who's eating that free or skimming the cash off someone else's meal sees that as \$10 the company is getting. What they don't factor, because they don't know, is that it costs us \$6 for the ingredients, \$1.50 for the wages to serve the meal, another \$1.75 for insurance, licenses, lighting, marketing, whatever. Of that \$10 you may get 75 cents down to the bottom line. They steal five of those dollars, you're not \$5 ahead, you're \$4.25 in the hole, you see? If all your employees ate a hamburger and had a soda every day and never paid, that's a huge cash loss.

This starts to get into something that's important, the mind-set of the person stealing, because they're probably thinking what I just said, "This big company isn't going to miss one burger."

The rationalization process is so deep. Maybe you can't believe the things people will do or say to justify their actions. Not many people, when confronted, are going to step up and say, "I did it and I was wrong." But that's life. You've got to understand that it makes sense to them, even if it makes no sense to you. You have to operate on the premise that there's always a need, and if we supply the opportunity, we're going to get beat.

There's something empathetic about the way you say that, as if you understand, or at least accept, that this impulse to rationalize theft is part of life.

It comes down to people. Not everyone is dishonest, but for some portion of the population, it's part of survival. This industry, there's a lot of work that goes into it. A lot of luck too. You don't always have control over hires. I think our people understand that. They do a good job with it. You know there are no guarantees, but as long as you're working together under sound policies, and you minimize opportunities, you hope that your losses are minimal.

What we're really talking about is the classic fraud triangle. You've accepted the rationalization some people will have. You

know they have motivation. All that's left is the opportunity.

And opportunity is provided when you fall down on your procedures.

Take cash handling. It's more of the same strict policy focus: You count cash in a locked room. The count is verified independently. Cash is put in tamperproof bags. When delivering a cash deposit, the bags are concealed and those deposits are always, always done during daylight hours. The concept is simple: The fewer people who have access, opportunity, the less problem you have. And people won't think to steal if they never see anything to be stolen. They never see the opportunity.

None of that is particularly high-tech.

Some of our lowest-tech policies are most effective. When you bleed the register for instance, you put the money in an envelope and seal it. Write your name across the back so that someone trying to get at that money has to break the seal and then replace the envelope with a new one and try to forge your name. That's not easy to do, so now they'll think twice about trying.

What other low-tech loss prevention techniques are you fond of?

We require employees to break down boxes, and this alone has helped minimize loss from freezers and anterooms (where ice cream and produce are stored). No boxes to put stuff in, no theft. But one of my favorites—if you ever go into the back of a restaurant you'll see a garbage bucket with a big magnetic bar running across the top. That one magnetic bar creates huge savings; it catches silverware that would otherwise [accidentally] be thrown away. I love it because it saves tons of money on accidental loss while allowing the servers to spend the time serving the customers [instead of] sorting silverware.

Armed robbery is a big concern.

Armed robbery is the most dangerous thing we face in this industry. What I tell employees is: You offer no resistance. The longer [the robber] is in there, the more opportunity there is for something



to go terribly wrong. Someone doing an armed robbery is by definition not thinking straight. Give them the money and get them out. Then, watch as they leave, trying to get as much detail as possible. Where did their head reach at the door, what were they wearing? Once they're gone, lock the door. Then, don't huddle up to discuss. When you huddle up and talk about what just happened, the strong personalities tend to dominate the conversation regardless of the accuracy of their information. Let the investigators come in and interview each person. They will get a much more detailed portrait of the event that way.

Does security have a say in restaurant design?

From a security standpoint, we have one design rule: Nothing's hidden. Everything is open, visible and well-lit. No curtains. A lot of glass. When the sun goes down, I tell them, the drapes go up. Because if you can't see out, the police can't see in. People, potential customers, also like to see in, so no ads on the windows. I tell supervisors to show activity. A bad guy is looking for a place where there's one person sitting

there reading a book. The register stays up front and open, the employee using it is in full view of everyone, which helps prevent insider threats from becoming a problem. The take-out area looks right through the restaurant. What we're doing is eliminating the opportunity to get out of sight.

Does the marketing group ever raise a fuss about the limitations—not being able to put ads in the windows, say?

Marketing understands the limitations on advertising. They respect our concerns.

Do you see anything happening in loss prevention today that concerns you?

I've been around a long time. I've seen a lot of people fail in security by taking the wrong approach, by thinking they know everything there is to know. The truth is, we all learn every day. A good investigator knows where to go for expertise. Today, it seems like everyone feels above that. More and more they think they don't need others. Come on. If I don't rely on others' expertise, I'm nowhere. ■

Send feedback to Senior Editor Scott Berinato at sberinato@cxo.com.

LOpht

IN TRANSITION

Most of the '90s hacking group have emerged in legitimate roles. Was their work ultimately boon or bane for security? By Michael Fitzgerald

Brian Oblivion. Kingpin. Mudge. Space Rogue. Stefan von Neumann. Tan. Weld Pond. That's how the hacker group called the LOpht appeared before the Senate Subcommittee on Government Cybersecurity on May 19, 1998. They said, among other things, that they could take down the Internet in 30 minutes. The senators listened closely and afterward praised them effusively.

It was a landmark moment for hackers, shunned, derided and loathed by the technology industry. And it was a landmark for the LOpht too. Though the group was already known for its vulnerability disclosures, for the Hacker News Network, for tools like the hash cracking tool LOphtCrack, now "everybody [in the hacking community] wanted to be the LOpht," remembers Jeff Moss, founder of the Black Hat and Defcon security conferences.

Not bad for a group that got its start when someone's wife said it was time to get his computers out of the bathtub.

The LOpht shaped the way disclosures are handled and helped force vendors like Microsoft to change the way they address soft-

ware security flaws. There's no question, either, that by raising the visibility of security problems, the group spurred companies to begin paying more attention to security. "You knew you'd better rattle your own doorknobs before the hackers did," says John Pescatore, a longtime information security analyst at Gartner.

Some think, though, that visibility has hurt software security. "They were the Led Zeppelin of gray hat hacking," says Marcus Ranum, who is credited with creating the first commercial firewall product and is now CSO at Tenable Network Security. "By releasing gray hat tools and techniques they were able to get a tremendous amount of attention. And they opened the floodgates for all the bottom feeders that followed them."

Ironically, it was Ranum himself who helped give the LOpht credibility. As CEO of NFR, which made software to find intruders on corporate networks, Ranum used the LOpht's vulnerability research to strengthen his product, and hired the LOpht both to do a code review and to write modules for his product, giving the group a legitimate corporate client to tout. He says he consid-

ers the LOpht members his friends and says they are "great guys." But he thinks those who have followed them find vulnerabilities almost as a way to blackmail corporations.

IN THIS STORY The impact and current whereabouts of a famous hacker ensemble

He blames the LOpht, saying, "They have changed the industry for the worse."

NOTHING IN the LOpht's emergence from Boston's bulletin board community in 1992 suggested it would achieve any more notoriety than other hacker collectives of the day. Brian Oblivion, a hacker with strong interests in radio communications, founded the group. Oblivion declined to be interviewed for this article, saying via Space Rogue that he was too busy. Chris Wysopal, who joined the LOpht in late 1992 as Weld Pond (a handle chosen by pointing at random at a map of the Boston area, because the bulletin board The Works forbade members to use real names), says that Oblivion "had so many computers in the bathroom that his wife couldn't use it anymore." She gave the group space in the South End artist's loft where she made hats. And for several years, the LOpht was just a place for Oblivion and his friends to hang out after work and store their growing collection of computing equipment.

Among those friends were Space Rogue and a teenage hacker and skateboarder named Joe Grand, who went by the handle Kingpin (named for the bolt that runs through the truck, or axle, of a skateboard).

Grand calls from the road. He's often on the road, literally—he is a triathlete good enough to have a sponsor. He's 31 now and runs his own San Diego design shop, Grand Idea Studio, which has designed RFID and GPS modules for Parallax, an in-game videocamera for Gamecaster, and his best design yet, a video game accessory that he has licensed but can't talk about.

Grand, an electrical engineer, has also written two books on hardware hacking and is a technical adviser to *Make* magazine. If all goes well with a pilot he's recently shot, this fall we'll see him on an engineering show on the Discovery Channel. Yet he's nostalgic about the LOpht.

"I'm having a really hard time with realizing that I'm twice as old as when I joined the LOpht," he says. "We did so many great things—what can I do to top that?"

THE LOPHT originally built a network so they could play *Doom* against each other. But they got more serious in 1994 and 1995, shedding some members and adding others with specific technical skills that complemented the group. They moved to a larger space in Watertown, Mass.

Excepting Grand, who was still in high school, all of the LOpht held various day jobs, often working together at places like Comp-

USA, Massachusetts General Hospital or BBN Technologies, the fabled research lab (Weld Pond, Brian Oblivion, Mudge and Silicosis all worked there at some point). They kept their identities hidden, in part to keep their day jobs. Everyone in the hacking community knew Dan Farmer had been fired from his job for releasing the Satan network analyzer. But the group wanted to turn the LOpht into a day job.

The charismatic, long-tressed Pieter "Mudge" Zatko had emerged as the group's public face, if not its de facto leader. He developed, along with Wysopal, LOphtCrack, a tool that revealed weak passwords. Released in 1997, it's still available on some websites today. "Back then, the companies would pretend [vulnerabilities] weren't real," says Bruce Schneier, the noted cryptographer and CTO of BT Counterpane. Schneier says the LOpht's ability to build tools like LOphtCrack forced vendors to address security problems. "That's the reason we have more secure software today. If it wasn't for that, Microsoft would still be belittling, insulting and suing researchers," he says.

By late 1998, the LOpht was actively trying to attract venture capital and turn itself into a real business—it had pushed out Stefan von Neumann and a couple of other short-lived members, and hired Christien Rioux (known as Dildog) and Paul Nash (known as Silicosis) to support LOphtCrack and do custom work for companies like NFR. The LOpht was not the first group of hackers to offer professional services or tools, but even in the giddy late 1990s, hackers still had an unsavory reputation. Finally, @stake, a security consulting firm, came to the group with \$10 million in VC money and told the LOpht it could continue its research. The members voted to join it.

Even so, that merger, announced Jan. 10, 2000, marked the symbolic end of the LOpht. Over the next few years, its members were fired or drifted away, and @stake itself was gobbled up by Symantec in 2004. The only member of the LOpht still there is Nash. The transition was particularly difficult for Zatko, who spent six months on disability and left @stake after just two years.

TODAY, ZATKO'S office at BBN is a rest area for sundry things. There's a dead computer on a chair, and a working circa-1940s polygraph machine on a table. In a corner are two fishing rods and an antenna, part of an impromptu communications experiment. There's a guitar signed by one-time porn stars Barbara Dare and Jamie Summers. A bound copy of the LOpht's testimony in front of the Senate is on a shelf. On one wall hangs a picture of him



GLORY DAYS: Pieter "Mudge" Zatko talks to a Senate committee about cybersecurity in 1998.



They were pointing out that **the emperor has no clothes on, and nobody wants to hear that, but they did it in a tasteful way that made people listen. They made a difference.**

—PETER NEUMANN, PRINCIPAL SCIENTIST, SRI

with President Bill Clinton and Vinton Cerf, in which Zatko's light brown hair is still rock-star length. It's short now, parted in the middle. He has a goatee and wears glasses. He's sore from a boxing workout the night before, a reminder that he's in his late 30s.

Zatko says he can't talk about what he does at BBN, other than to say it's security-related and for some unmentionable three-lettered government agencies. He also says he returned to BBN, which employed him in the 1990s, before the LOpht was his job, in part because BBN told him there could be no publicity about the projects he was working on. "That was attractive as hell," he says.

But Zatko can't seem to stay out of the spotlight. He is the obvious model for "Soxster," one of the main characters in former cyberczar Richard A. Clarke's new novel, *Breakpoint* (the LOpht itself appears as "the Dugout"). And he acknowledges that he still "wants to make a dent in the universe," the old motto of the LOpht.

After an hour of talking about the LOpht, Zatko suggests a tour of the older parts of the BBN laboratory in Cambridge, dating from when it was an acoustics consultancy. He shows off the silent room, the amplification room, the sonar tank, the place where it developed Boomerang—a technology being used in Iraq to help find snipers—and he talks about how much he likes the variety of the cool ideas BBN pursues.

"Originally, the LOpht was meant as a microcosm of here," he says, with a wistful expression.

THE SPIRIT of the LOpht lives on most directly at Veracode, the security software company started by Wysopal and Rioux after they left Symantec in 2005. The company launched at the RSA Security Conference in February.

Wysopal post-LOpht helped codify responsible disclosure policies and establish the Organization of Internet Safety, and while starting Veracode he also managed to be lead author of *The Art of Software Security Testing*, published in December 2006.

Wysopal, at a rangy 6 foot 2 inches, was the tallest member of the LOpht and the oldest (he's now 41). Rioux (whose handle Dildog was the original name *Dilbert* creator Scott Adams gave to Dogbert) was the shortest and youngest (now 29).

In early January, sitting in the conference room at Veracode, the two play Click-and-Clack about their time at the LOpht, and the purpose of Veracode, which in a real sense extends the LOpht's

mission: to make software more secure, in this case by offering a Web-based service that automatically checks software for security flaws, via a clever—and patented—technique for data flow modeling and modeling control flow analysis developed by Rioux.

Told of Ranum's comments, Rioux makes a slight grimace. "The days are over when we should be flinging mud over the Internet about vulnerabilities," he says.

Veracode has pulled in \$19.5 million in capital from Polaris Venture Partners, Atlas Venture and .406 Ventures. While it has competitors, such as Coverity, Fortify and Ounce Labs, Veracode's approach is "a cool spin" on existing security technology, according to Gartner's Pescatore.

Both Wysopal and Rioux believe Veracode is ready to sharply reduce the world's total number of software vulnerabilities.

THE LOPHT, then, are all now unquestionably legitimate, and their evolution serves as a metaphor for the security business, which is now mainstream. Companies like Microsoft and Oracle have developed methods to take care of vulnerabilities, and the LOpht deserves some credit for that turn of events. While the disclosure wars are again raging, thanks to bug-a-day campaigns and other ploys by the hackers of today, the LOpht's overall impact on corporate security has been positive, say many, including Howard Schmidt, who knew the LOpht both in his role as a computer forensics investigator at the Air Force and as CSO at Microsoft.

Still, some vendors continue to try to shove security issues under the rug, and there is no question that more of the Internet is under attack today than ever before. So what of that?

Peter Neumann (no relation to the LOpht's Stefan von Neumann) is 74 and still a principal scientist at SRI, working on security issues. He also testified before the Senate subcommittee on that day in May 1998. He says security vulnerabilities are a part of a much bigger set of problems that have existed for 40 years and probably will exist 40 years from now. But he chuckles when asked about the LOpht, saying, "They were pointing out that the emperor has no clothes on, and nobody wants to hear that, but they did it in a tasteful way that made people listen. They made a difference." ■

Michael Fitzgerald is a freelance writer based near Boston. Send comments to csoletters@cxo.com.

The CSO Executive Seminar Series on

IDENTITY MANAGEMENT

Register today at www.csoonline.com/conferences.

The CSO Executive Seminar on Identity Management will tackle this issue by examining the demands placed upon organizations, and how those demands can be addressed with enterprise identity management solutions. With the help of leading experts and practitioners we'll examine the benefits and challenges, review an implementation case study, and explore the business case for adopting these solutions.

WHO SHOULD ATTEND

CSOs, CPOs, CISOs, Security & Privacy Protection Managers, Legal Counsels and others who are charged with protecting documents and files containing identification information.

Government and non-profit officials who prepare their organizations for security issues.

BENEFITS OF ATTENDING

A 360 degree view of identity management including:

- Key identity management implementations
- Building a business case for identity management
- Navigating the roadblocks to success

Visit www.csoonline.com/conferences to view the entire agenda.

SAN FRANCISCO, CALIFORNIA

Thursday, June 14, 2007

7:30am-3:30pm

Ritz Carlton Hotel

NEW YORK, NEW YORK

Wednesday, June 20, 2007

7:30am-3:30pm

Grand Hyatt New York

Space is limited. Register today at:
www.csoonline.com/conferences
or for more information call
800.366.0246

Platinum Sponsor:

Novell

Produced by:

CSO
The Resource
for Security
Executives



THE RESOURCE FOR SECURITY EXECUTIVES

Sales and Services

CSO Sales Offices

President and CEO
Michael Friedenbergs • 508 935-4310

Publisher
Bob Bragdon • 508 935-4443

Senior Ad Sales Associate
Christine Hopkins • 508 988-7836

Eastern Territory

East Coast Regional Manager
Roz Burke • 508 935-4163

Western Territory

Senior Regional Sales Manager
Ai Collins • 415 975-2686

Regional Sales Manager
Drew Seifried • 206 245-3328

Integrated Media and Online Sales

Online Regional Sales Managers
Tina Dudarevitch • 718 279-2396
Lori Kehoe • 415 978-3329

Online District Sales Manager
Sara Mascall • 415 978-3385

Manager, Online Account Services
Danielle Tetreault • 508 988-7969

Online Account Services Specialist
Valerie Sumner • 508 988-7877

Online Ad Sales Associate
Devon Slattery • 415 975-2687

Online Advertising Specialist
Irina Gabechiia • 508 935-4414

Online Account Services Coordinator
Hayley Nickerson • 508 988-7819

Custom Solutions Group

Vice President
Matt Avery • 508 935-4796

Executive Editor
Tom Field

Managing Editor
Jim Malone

Associate Editor
Anne Taylor

Senior Project Manager
Amy Greenleaf

Project Managers
Karen Capland, Amy Freeman

CSO Executive Council

Managing Director
Bob Hayes

VP, Research and Product Development
Kathleen Kotwica

Director, IT and Product Technology
Greg Kane

Operations and Production Specialist
Jayne Marcucella

Member Services Manager
Elizabeth Lancaster

Production

VP/Manufacturing
Chris Cuoco

Production Manager
Heidi Broadley

Associate Production Manager
Lisa M. Stevenson

Executive Programs

VP, Executive Programs
Ellen Daly

Director, Business Development
John Vulopas

Director, Event Marketing
Mary Conroy

Director, Event Operations
Deb Begreen

National Sales Manager
Per Melker

Senior Conference Producer
Judith Kittredge

Event Planner
Sarah Reagan

Event Coordinator
Bethany Whiffin

Registration Specialist
Cress O'Brien

Client Services Specialist
Erica Foster

Sales Associate
Nicole Blackburn • 508 935-4154

Marketing

Sr. Director, Marketing Communications
Sue Yanovitch

Sr. Marketing Communications Specialist
Susan Murray

Marketing Communications Specialist
Lynn Holmlund

Circulation

Senior VP/Circulation
Carol A. Spach

Subscription Services Supervisor
Tina Pescara

List Services

Contact Paul Capone of IDG List Services at
508 370-0865 or pcapone@idglist.com.

Reprint Services

For article reprints (100 quantity or more),
please contact Keith Williams at PARS
International at 212 221-9595, ext. 319,
or e-mail keith.williams@parsintl.com.
For further sales information, visit
www.csoonline.com/reprints/index.html.

CSO Contact Information

Editorial/Advertising/ Business Offices

492 Old Connecticut Path, P.O. Box 9208,
Framingham, MA 01701-9208
Main phone number: 508 872-0080

Postal Information

CSO (ISSN 1540-904x) is published
monthly by CXO Media Inc., 492 Old Con-
necticut Path, P.O. Box 9208, Framingham,
MA 01701-9208. Periodicals Postage Rate
at Framingham, MA 01701, and at additional
mailing offices. Canadian Publications Mail
agreement number 1902075. CANADIAN
POSTMASTER: Please return undeliver-
able copy to P.O. Box 1632, Windsor, ON
N9A 7C9.

Permissions

Copyright 2007 by CXO Media Inc. All
rights reserved. Reproduction of material
appearing in CSO is forbidden without
written permission. Send requests to Yadira
Pizarro, PARS International, 212 221-9595,
ext. 231, or e-mail yadira@parsintl.com.

Photocopy Rights

Permission to photocopy for internal or per-
sonal use or the internal or personal use of
specific clients is granted by CSO for users
through the Copyright Clearance Center,
provided that a fee of \$3.50 per copy of the
article is paid directly to Copyright Clear-
ance Center, 222 Rosewood Drive Danvers,
MA 01970. www.copyright.com. Please
specify: ISSN 1540-904x. Permission to
photocopy does not extend to contributed
articles followed by this symbol: ‡.

Subscriptions

Address inquiries to CSO, P.O. Box 3482,
Northbrook, IL 60065; 866 354-1125.

CSO is free to qualified information
executives. To all others the one-year
basic rate is \$70 for the United States and
Canada, \$95 to foreign countries (payable
in U.S. funds only). The single copy price
is \$9 to the U.S. and Canada and \$15

International. Please allow four to six weeks
for new subscriptions to begin.

Change of Address

Go to www.ameda.com/custsrv/cso and
follow the online instructions.

Postmaster

Send change of address to:
CSO, P.O. Box 3482, Northbrook, IL 60065.
Printed in the USA.

Index of Companies and Advertisers

Company Index

406 Ventures	30
American Express Co.	16
Atlas Venture	30
BBN Technologies	30
CheckFree Corp.	16
Chevron Corp.	16
Chief Security Officers	16
ChoicePoint	16
CommTouch Software Ltd.	7
CompUSA Management Co.	30
Counterpane Internet Security Inc.	30
Dow Jones & Co. Inc.	16
DriveSavers Data Recovery	7
DuPont	7
Federal Trade Commission	7
Friendly Ice Cream Corp.	4, 26
Gartner Inc.	16, 30
Grand Idea Studio Inc.	30
Harvard University	14
Home Depot U.S.A. Inc.	36
Honeywell International Inc.	4
JCB International Credit Card Co. Ltd.	16
Los Angeles County Economic Development Corp.	7
Marriott International Inc.	16
Mastercard	16
Merchant Risk Council	16
Microsoft Corp.	14, 30
Morgan Stanley Co.	16
New York Times Co., The	7
One Laptop Per Child	14
Pay By Touch	16
PayPal	16
PCI Security Standards Council LLC	16
Polaris Venture Partners	30
Red Hat Inc.	14
Royal Ahold	16
Sony Corp.	7
Sophos Plc.	7
SRI International	30
Stop & Shop Supermarket Co.	16
Symantec Corp.	22, 30
Tenable Network Security Inc.	30
TJX Companies Inc., The	7, 16
Turner Broadcasting System Inc.	7
Veracode Inc.	30
Visa International Service Association	16
Advertiser Index	
BigFix Inc.	5
CA	C4
CXO Media Inc.	13, 23, 33, 35
Executive Women's Forum	34
HID Corp.	6
Intel Corp.	C2
LURHQ/SecureWorks	3
Oracle Corp.	9
Tumbleweed Communications Corp.	C3
Tyco Fire & Security	11

Women of Influence Awards

CALL FOR NOMINATIONS

Nominate your peers, clients and
customers for the Women of
Influence Awards. Co-presented
by Alta Associates and CSO
magazine, the awards honor four
women for their accomplish-
ments and leadership roles in
the fields of information security,
risk management and privacy.
Winners will be announced at an
awards ceremony during the
Executive Women's Forum.

Nomination form available at:
www.infosecuritywomen.com

**NOMINATIONS MUST
BE SUBMITTED BY
AUGUST 1, 2007**

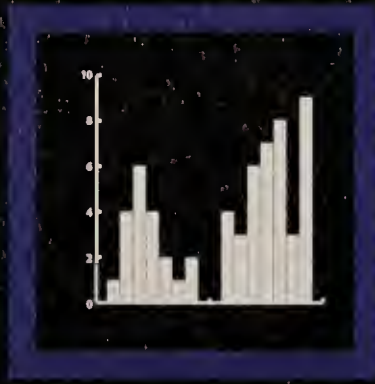
Media sponsor & awards co-presenter:



Forum host & awards co-presenter:



CSO Perspectives



The Business Case for Security

How to Plan, Deliver, Measure and Communicate

Thank you to the 2007 sponsors:

Platinum:



Silver:



OUNCE LABS

Bronze:



Brabeion
IT Risk & Compliance Management



Join us for one of the upcoming CSO Executive Seminars on

Privacy

Thursday, May 17, 2007
Chicago, Illinois
Hyatt Regency McCormick Place

Identity Management

Thursday, June 14, 2007
San Francisco, California
Ritz Carlton Hotel
and
June 20, 2007
New York, New York
Grand Hyatt

Space is limited. Register today at www.csoonline.com/conferences or for more information call 800.366.0246.

Produced by:

CSO
The Resource for
Security Executives

debriefing

Smuggler's Notch



Stashed and Found

A recent report about large quantities of illegal drugs found in vanities sold at Home Depot got us thinking about other places criminals try to hide their goods. Headlines and news clips from around the world confirm that stashing drugs is indeed a creative enterprise:

Guard accused of smuggling pot hidden in cannoli

Police report that they found a stash of pot hidden in a roll of tummy flab

U.S. Marshals sold pot-laden car; unwitting buyer arrested for pot hidden in bumper

Pot hidden in bus headed for Special Olympics

Pot hidden in cargoes of limes, raspberries, lettuce, tomatoes, mangoes, squash, onions, pineapples, bell peppers, jalapeños and jicama, cantaloupes and bananas

683 pounds of pot hidden in two air conditioner crates

Marijuana hidden in a meat freezer beneath 10 pounds of frankfurters

An undercover agent bought 14 kg of marijuana hidden in cheese wheels from an Old Colony Mennonite

Peru drugs hidden in giant squid

Man in China's Yunnan province arrested for attempting to smuggle drugs hidden in the stomachs of ducks

Drug ring used tiny spaces in computer hard drives to smuggle heroin and cocaine

Customs officers allegedly discovered drugs hidden in PC monitors

Heroin traffickers sew drugs into puppies

Drugs hidden in child's mitten

A Bradford [England] man has been jailed for plotting to throw drugs hidden in tennis balls into the prison where his brother is serving a 12-year sentence

Heroin was found hidden in the covers of children's encyclopedias

Customs officials swooped on a man trying to smuggle cocaine—hidden in his false leg

More than five tons of drugs found hidden in consignment of dog food

Drugs hidden in grindstones seized

Drugs found in counterfeit lager cans concealed among trays of the genuine article

Cocaine was found inside dummy avocados—made of papier-mâché—imported with normal shipments

Drugs hidden in grilled bird

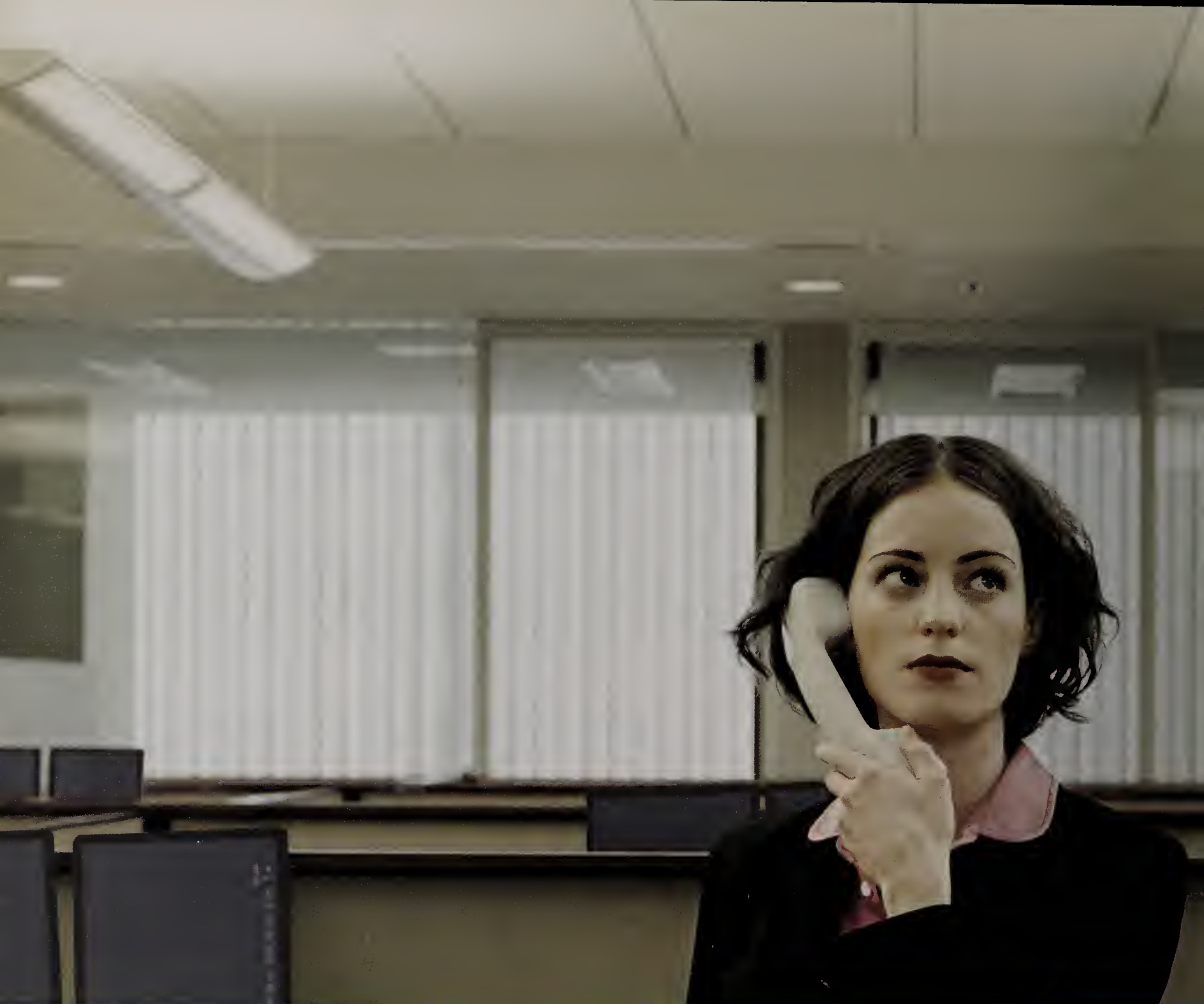


There's an easier way to secure your messaging. *(Without resorting to dubious methods.)*

There isn't much IT managers won't try when it comes to protecting email and file transfers. But drastic measures (even the creative ones) run the risk of wasting valuable resources and hindering employee productivity. Tumbleweed delivers serious protection, simply. With a product suite that's quick to deploy, easy to manage and intuitive to use, your messages are guaranteed a safe flight.

www.tumbleweed.com/easierway

 **Tumbleweed®**
Messaging. Secure and Simple.



Why can she see everyone's salary, but can't confirm her vendor's payment?

Keep information secure with Identity and Access Management (IAM) solutions from CA. Hold on. Employees with access to information they should never see? And no access to the information they need to do their job? When you're adding employees and changing their responsibilities, it's bound to happen. Unless you have Identity and Access Management solutions from CA. Our industry-leading IAM gives you enterprise-wide security and control.

It's what's made CA the IDC worldwide market leader in IAM six years running, since 1999.* How'd we do that? Well, we're looking at IT from a whole new perspective. It's unified and simplified, it's security without question. And it's all at ca.com/iam.



Transforming
IT Management

* IDC, Worldwide Hardware Authentication and Identity and Access Management
2005 Vendor Shares, Doc #203296, Sep 2006.
Copyright © 2007 CA. All rights reserved.